State of Arkansas
Office of Information Technology
124 West Capitol Avenue Suite 990 Little Rock, AR 72201
Phone 501-682-4300 Fax 501-682-2040
http://www.cio.arkansas.gov/techarch

Agency #200.00

DRAFT Standard Statement – Wireless Security

Title: Wireless Security

Document Number: SS-70-010

Effective Date: x/x/2007

Published by: Office of Information Technology

1. Purpose

Wireless technology gives users the ability to access data and applications from more locations in a cost effective manner, but wireless technology also presents problems in terms of security. All information assets handled by computer systems must be adequately protected against unauthorized modification, disclosure, or destruction. For these reasons, appropriate security measures are essential when deploying wireless technology *with access to the state network*.

2. Scope

This standard statement applies to all state agencies, administrative sections of institutions of higher education, boards and commissions.

3. Background

The Arkansas Information Systems Act of 1997 (Act 914, 1997) gives the Office of Information Technology the authority to define standards, policies and procedures to manage the information resources within the state. This is accomplished through work with a multi-agency working group known as the Shared Technical Architecture Team.

In addition, Act 1042 of 2001 states that the Executive Chief Information Officer oversees the development of information technology security policy for state agencies.

4. References

4.1 Arkansas State Government Information Resources Security Policy Guidelines

4.2 *Act 914 of 1997*: Authorized the Office of Information Technology (OIT) to develop statewide policies

4.3 *Act 1042 of 2001*: Authorized the Executive CIO to develop security policy.

4.4 Encryption Standard: http://www.cio.arkansas.gov/techarch/indexes/standards.htm

5. Standard

5.1. All configuration parameters (such as Service Set Identifier (SSID), keys, passwords, etc.) of Wi-Fi access points or bridges that can be changed from the default manufacturer settings shall be changed from the default. The beacon interval on the these Wi-Fi access points should be set to the longest interval possible. Where applicable, the new settings should be complex.

5.2. Wireless hotspot networks may exist on the state network if and only if the following are met:

5.2.1. The Service Set Identifier is changed to one which appropriately identifies the wireless network as a hotspot environment.

5.2.2. A secure method exists to identify and authenticate users of the hotspot environment such as a captive web portal. Appropriate audit logs containing IP address, login id, and logon/logoff date and time stamps should be maintained based on the organization's data retention policy.

5.2.3. Systems or applications which contain data which is classified by the SS-70-001 Data and System Security Classification Standard as being Level B - Sensitive, Level C - Very Sensitive or Level D - Extremely Sensitive must have appropriate access controls (firewall rules, router access control lists, and similar measures) that disallow wireless hotspot users from directly accessing the system or application.

5.2.4. Users of the hotspot environment which require access to systems or applications classified Very Sensitive or Extremely Sensitive must use appropriate technology such as VPN, secure shell, SSL/TLS encrypted webpages and similar authenticated and encrypted technology to access these resources in accordance to SS-70-009 Remote Access standard and the SS-70-006 Encryption standard.

5.2.5. Appropriate warning banner is presented to authorized and unauthorized users of the hotspot environment captive portal in accordance to SS-70-003 Warning Banner. Hotspot users must be given opportunity to view any appropriate "acceptable use policy" and must agree to this policy as a part of authenticating via the captive portal.

5.2.6. Access to any Internet resources are denied to hotspot users until the authenticated to the wireless network through use of appropriate firewall or other access control mechanisms.

5.3. Covered entities which use wireless networking in a non-hotspot environment must adhere to the following.

5.3.1. Service Set Identifier must not contain information relative to agency location, mission, or name.

5.3.2. Wi-Fi equipment shall be configured for infrastructure mode only.

5.3.3. All wireless transmissions between a state network entity's wireless access point or bridge and clients shall be encrypted utilizing the WPA protocol at a minimum to prevent unauthorized access to the state network.

5.3.4. WEP (wireless encryption protocol) shall not be utilized due to its multiple security flaws.

5.3.5. Wirelessly transmitted data and credentials granting access to state resources are subject to SS-70-009 Remote Access and SS-70-006 Encryption standards.

5.4. Covered entities will search for and disable rogue Wi-Fi access points to the state network quarterly, at a minimum.

5.5. Covered entities utilizing wireless technologies shall establish a policy to ensure compliance with the state wireless security standard.

5.6. Wireless networks that covered entities may use that are separate from the state network are not subject to this standard. Clients, however, must still adhere to SS-70-009 Remote Access and SS-70-006 Encryption standards when accessing Level B, C or D data from these outside environments.

5.7. Bluetooth wireless devices must be secured to the extent configurable between the devices involved.

6. Procedures

The State Security Office reserves the right to audit for compliance with this standard. Furthermore, the State Security Office has the right to grant an exception or exclusion to any part of this standard. The Arkansas Division of Legislative Audit also audits for compliance with this standard.

7. Revision History

Date	Description of Change
x/x/2007	Original Standard Statement Published

8. Definitions

8.1 Bluetooth

Bluetooth is a computing and telecommunications industry specification that describes how mobile phones, computers, and personal digital assistants (PDAs) can easily interconnect with each other and with home and business phones and computers using a short-range wireless connection.

8.2 Hotspot

A public or semi-public wireless local area network (WLAN) that provides Internet access to subscribers

8.3 Rogue Access Point

Unauthorized wireless device allowing access to the state network

8.4 SSID (Service Set Identifier)

A service set identifier (SSID) is a sequence of characters that uniquely names a wireless local area network (WLAN). This name allows stations to connect to the desired network when multiple independent networks operate in the same physical area.

8.5 State Network

The state core information technology infrastructure serving Arkansas agencies, boards, commission, public schools, institutions of higher education, libraries, and other public organizations with Internet connectivity, data processing and transmission, video conferencing and telecommunications

8.6 WEP (Wired Equivalent Privacy)

WEP (Wired Equivalent Privacy) - WEP is an optional privacy protocol originally specified in the IEEE 802.11 (802.11 legacy) standard that is designed to provide a level of security and privacy comparable to what is usually expected of a wired LAN. Weakness in the design make this protocol unsuitable for use in environments which must protect sensitive data.

8.7 Wi-Fi

A term used to describe the underlying technology of wireless local areal networks (WLAN) based on the IEEE 802.11 set of specifications and is used interchangeably with the term wireless. Wi-Fi refers to any individual standard or the collection of all standards within the 802.11 family such as 802.11a, 802.11b/g, 802.11i or 802.11n.

8.8 Wireless

Wireless LAN (local area network) data access technology including the following protocols: 802.11 series and Bluetooth that accesses state information technology resources.

8.9 WLAN (wireless local area network)

A communication system that enables mobile users to connect to a wired network through a wireless (radio) connection, often implemented as an extension to wired LAN. WLAN’s are typically found within a small client node, dense locale (e.g. a campus or office building), or anywhere a traditional network cannot be deployed for logistical reasons.

8.10 WPA (Wi-Fi Protected Access)

WPA is a security standard for users of computers equipped with Wi-Fi wireless connection. It is an improvement on and is expected to replace the original Wi-Fi security standard, Wired Equivalent Privacy (WEP). WPA provides more sophisticated data encryption than WEP and also provides user authentication.

9. Related Resources

9.1. FCC Wireless Website: http://wireless.fcc.gov/

9.2. SANS website: www.sans.org

9.3. Bluetooth website: www.bluetooth.com

9.4. Wi-Fi Alliance website: www.wifialliance.org

10. Inquiries

Direct inquiries about this standard to:

Office of Information Technology
Shared Technical Architecture
124 W. Capitol Ave., Suite 990
Little Rock, AR 72201
Voice: 501-682-4300
FAX: 501-682-2040
Email: sharedarchitecture@arkansas.gov
OIT standards can be found on the Internet at: http://www.techarch.state.ar.us